Presenter: Michel Coulombe, CSIS Director
Audience: CEO Advisory Group
Topic: Cyber Security
Word Count: 5361 (~ 45 minutes, ~ 15 Minutes of Q&As)

Purpose: To provide an integrated Government of Canada threat brief on cyber security threats and trends, including to Canadian interests abroad and threats emanating from the travel of Canadian persons.

Cyber Security Presentation to the Chief Executive Officer Advisory Group

- **(U) Good afternoon ladies and gentlemen. I am here today to share some of our current insights on cyber security threats and trends as well as to speak to how these hostile activities can affect the businesses you represent.**

- **(S) It used to be thought that only certain sectors, such as high tech, aerospace, and military-based industries were at risk. That simply is not true today. Cyber-based threats are ubiquitous and can affect Canadian industry ranging from high tech to resource extraction to agriculture. We have seen now that any business with a certain level of expertise can and will be exploited by actors unconcerned with the laws governing intellectual property, trade, and commerce.**

- **(U) These threats are also global. They do not end at the shores of Halifax or Vancouver – they will follow your companies and their offices abroad, where Canadian law and security agencies have limited reach.**

- **(U) Today, I will make an effort to be as transparent as possible on the threats we face and the tactics of our adversaries and competitors. I would ask, however, that you treat this information as sensitive and respect the SECRET-level classification of today's briefing.**

- **(S) Ladies and gentlemen, what we are witnessing today is the creation of a new threat environment. Cyber power has become a game-changer in defining global projection of power in the 21st century.**

The

evolution of this threat environment

Indeed,

- **(U) Cooperation with our corporate partners to face this cyber threat is vital for success given that the majority of Canada's critical infrastructure and intellectual property resides in the private sector.**

(U) Before discussing these threats, I would like to acknowledge that Canada's cyber security regime is a team effort and includes the Communications Security Establishment, Public Safety Canada, the RCMP, and CSIS, all of whom maintain dedicated units to countering cyber threats. Both Public Safety's Canadian Cyber Incident Response Centre and the Communication Security Establishment's Cyber Threat Evaluation Centre are

vital to improving the security posture for both government and private sector networks. Through the leveraging of each organization's unique mandates and expertise, the Government works to ensure that Canada's cyber space is safe and secure for Government, business, and its citizens.

- CSIS' role in Canada's cyber security regime, in accordance with its mandate, is to determine whether the cyber activities of individuals, organizations or groups constitute a threat to the security of Canada. With Service advice, the Government makes better, more informed decisions related to policy, response, investment and governance. The Service's cyber program is providing unique dividends to the Government and partners in the public and private sector across Canada. As well, the addition of our new threat reduction mandate through the recent passing of C-51 will certainly provide further opportunities to counter this threat. Ultimately, the Service's cyber programs will contribute to Canada's economic well-being and prosperity by making Canada's cyber space safer.

- (U) And keeping the cyber space safe and secure for Canadians and Canadian business is the ultimate goal. While no clear or reliable estimates exist, some have placed the global costs related to cyber security between $375 to $575 B USD annually, and potentially $12 B CDN annually in Canada. Clearly, cyber security isn't just about national security; it's about the economic security and continued prosperity of Canada and our way of life.

- (S) As internet connectivity expands into every corner of the globe, the threats will multiply,

- (S) During this past year,

- (S) On the technical side, internet connected home devices, cloud platforms and the commoditization of internet-enabled technology continues to evolve, improve, and expand. The heightened commercial value of security and privacy due to consumer demand have led to recent commitments from Apple and Google to improve device-based encryption and privacy settings.

- (S) All actors, both state and non-state, are becoming increasingly aware of the asymmetric opportunities presented by offensive cyber activities when used in conjunction with other programs, although clear international norms have yet to emerge.

- **(S) Exacerbating these security trends are social trends associated with today's technological revolution. For instance, many people today think nothing of geolocating themselves on Facebook and through dating apps. Pictures, interests, and relationships are shared with little thought or care. Just as private companies use such data to build profiles for advertisers to market products directly to consumers, cyber actors too can use such information and techniques to their advantage and well beyond the arguably benign uses of online niche marketing.**

- **(S)**

  . I will discuss this later in my presentation, with a particular focus on how it could affect the private sector if the threat evolves.

- **(S) I would like to now turn to state based actors,**

- **(S) But before we begin, we should also be clear – the cyber-based collection activities of our adversaries are not equatable to those of Canada and our closest allies.**

  the Canadian intelligence community does not collect intelligence in support of the specific interests of private businesses or industry.

- **(U) Canada's national security community conducts its activities within clear legal parameters and often through measures warranted by the Courts. Our key adversaries, as you may be aware, do, however, engage in espionage in support of their private industry..**

- **(S) In my discussions with my Government colleagues, I have always advocated for an "eyes-wide-open" approach I do not envy the decisions you must make in this regard. And, as members of the national security community, we realize that interacting with That said, we must do so knowing full well the inherent risks of such interactions.**

- **(S) In one instance, for example,**

- **(S)**

And, if ever you suspect illicit or compromising activities, please do report them to the appropriate authorities that are represented here today.

(S) In addition to pure cyber-based operations, traditional human source operations can be combined with cyber techniques for great effect.

As such, charges and further investigations were not pursued.

- **(S) In another example, recently,**

Unfortunately, one of the lessons learned in this case is that losses are not limited to what is actually compromised or stolen but include residual costs of repairing, restoring, and enhancing entire compromised IT systems to mitigate risks of future attacks. These losses may be minor compared to the significant opportunity costs associated with this theft.

The danger in using offensive cyber operations is that rules of escalation are not well established. As such, offensive cyber-attacks resulting in a loss of life could be construed as an act of war and likely to elicit a strong counter-attack.

- **(U) Non-aligned groups also constitute a threat to both government and corporations. Hacktivism groups, such as Anonymous have evolved to become more of a socio-political collective than a traditionally organized entity which is managed by a top-down hierarchy. Targets are chosen in order to promote the collective's social and political agendas. To date, Anonymous' cyber campaigns have focussed on perceived Internet censorship, alleged corrupt corporations and governments, alleged government infringement of human rights and freedoms, and perceived police brutality.**

- **(U) Of particular concern to the private sector, is the interest from such groups in damaging various governments' and corporations' public relations images in order to raise public awareness of perceived and alleged injustices.**

- **(S) While we have discussed state-based and non-aligned actors, I have not, as of yet, tackled terrorist groups' use of cyberspace. Largely,**

(S) **And frankly, it works.**

- (S) In addition, we have also seen growing interest from to engage primarily for the purpose of While some actors associated with may have the

- (S) That said, While we have yet to see this, it is certainly a growing concern as technology is pervasive and expertise becomes relatively easy to acquire.

- (S) Industries that could be targeted by offensive cyber operations are likely to include critical infrastructure with particular focus on areas where public safety could be compromised, such as transportation infrastructure. That said,

- (S) Such a development would be truly concerning, as terrorist actors do not respond to the same incentive mechanisms as most states, The community is actively monitoring for any such developments.

- (U) Turning now to cyber criminality, according to the RCMP, criminal networks are demonstrating strong cyber capabilities. At the transnational level there are organized crime networks that have capital estimated in the billions of dollars. Their financial position creates the opportunity for them to access the most advanced cyber capabilities normally associated only with nation states. Individuals participating in these networks have been known to hack into government systems to steal information, infect thousands of computers to steal data and/or launch further cyber-attacks, sell illicit drugs and guns through online criminal marketplaces, among other crimes.

- (U) Today, the expansion of online criminal marketplaces, including a growing service-based cybercrime industry, has emerged worldwide, providing the tools and technical expertise required for even amateur criminals to profit from cybercrimes like the theft, illegal sale and fraudulent use of compromised personal, corporate, and/or government data.

- (U) The RCMP, along with its partners, is also working to respond to the resurgence of Denial of Service (DoS) attacks of all sorts. Individuals or groups of criminals are targeting

corporations of all sizes in an attempt to extort money. Specifically, an entity identifying itself as DD4BC launched such a campaign that continues today. Its approach is to attack a target with a DoS, and subsequently send correspondence - in the form of an email, twitter messages - requesting the payment of a fee or the attack will increase. The amount demanded is usually in the range of 25 to 50 bitcoins - or $6675 to $13350 USD. This campaign has targeted several companies in Canada along with the U.S., U.K. Australia, France and several others. Given the scope of the attacks, the RCMP has partnered with key countries in an attempt to take action against DD4BC.

- (U) Formerly known as the Man-in-the-email scam, the RCMP is seeing a resurfacing of what is now referred to as Business Email Compromise fraud. This type of fraud targets wire transfer payments made to foreign banks. Fraudsters are using everything from simple social engineering ploys to more sophisticated email system compromises to convince an employee to execute a transfer to a fraudulently created bank account.

- (U) Frauds of all types are being reported to the Canadian Anti-Fraud Centre. In 2014, it received over 14,000 complaints of cyber-related fraud accounting for more than $45M in reported losses. As you can imagine the reality is these numbers are likely underreported and the true extent of victimization is much greater.

- (U) As the federal lead for cybercriminal activities, the RCMP focuses on incidents that have a national impact. For example, in December 2014, the RCMP charged the individual responsible for the well-known "Heartbleed" software vulnerability, which involved a malicious breach of taxpayer data at the Canada Revenue Agency (CRA). Primary charges involved one count of unlawfully obtaining a computer service and one count of unlawfully intercepting a computer system function. The suspect also faced 14 additional charges involving alleged hacks against the CRA, the University of Western Ontario, the London District Catholic School Board, and an offshore email service, among other victims.

- (U) The international nature of cyberspace, as you can imagine, presents challenges to law enforcement to obtain, exchange, and analyze vast amounts of digital data and evidence to successfully prosecute criminal cases with a cyber-nexus. With this in mind, the RCMP is pleased to be a part of the Joint Operational Resilience Management pilot project, which has brought together a multi-disciplinary team of financial sector representatives and the RCMP. Such endeavours will benefit Canadians by providing them secure environments to carry out their online activities.

- (U) Given both the national security threats and criminal activities just described, what can you as business leaders do to protect your employees and companies?

- (U) I will focus on two facets of this question today. The first in relation to travel abroad for business and the second in relation to protecting your offshore locations, often in less than hospitable environments.

- (S) We certainly recognize that business travel in a competitive global economy is a necessity. That said, there are some very practical steps you can take to ensure it is done as safely and securely as possible.

- (S) The significance of the knowledge you have must never be taken for granted. It is easy to think some of it is benign or even public.

  While perhaps a more important lesson for your junior employees, it is important for all employees to maintain their situational awareness in this regard.

- (S) It is important to realize that even before you leave to travel abroad,

  The best rule of thumb is to assume you are being targeted and adjust your behavior accordingly. On the cyber front, recognizing that conducting business on open platforms presents the greatest risk, travel preparation can involve some very common-sense tips.

- (S) First,

  While I understand such a motivation, you must realize that it could lead to greater compromise of sensitive data.

- (S) Second,

  While it is not a fail-safe approach, it will at least complicate and likely delay an adversary targeting you.

- (S) Third, do not use

  Similarly, do not accept such

  Accessing your

- (S) Fourth, when at all possible,

  You may even wish to

  That said, such devices are still at risk from malware or other exploitation techniques that could be surreptitiously installed.

- (S) For your background, CSIS is aware that foreign threat actors have a variety of tradecraft abilities,

- (S) These are not theoretical activities. We have seen them happen over and over again in our investigations.
- (U) As you are all aware, implementing best practices in relation to IT security is of course always advised. Seventy to eighty per cent of the cyber incidents that CSIS observes relate to known vulnerabilities for which there are known solutions. I would stress: Don't make it easy for competitors to acquire information easily. By imposing costs, companies can change the cost/benefit calculus and help forestall future attacks.
- (U) I know there was also some interest to discuss challenges associated with operating offshore, in particular the potential for increased risks to cybersecurity. In general, any operation or activity that lessens your direct control over information or property is at greater risk of theft and exploitation, especially when contracting out to third parties.
- (S) While the profit motive ensures a certain loyalty from

  There is simply no way to avoid this issue in countries where these practices are not only allowed but encouraged by the authorities
- (S) In addition, operating in foreign jurisdictions means you will be playing an "away game." State authorities will maintain intimate knowledge of the rules and the local players and how to circumvent or simply ignore legal restrictions to their advantage.

- (S) Unfortunately, there are no means to eliminate this risk. Instead, these risks will need to be managed and assessed continually, particularly through a careful examination on what information is shared to offices abroad. This includes the private information of customers, which could prove a valuable commodity for a myriad of reasons, including monetary and a further means to conduct espionage.
- To report any such incidents like I have described, all private organizations can contact the Canadian Cyber Incident Response Centre (CCIRC) at Public Safety. The CCIRC will provide you with regular reports on compromises and help you protect and mitigate against these threats. These services are provided to all Canadian organisations free of charge and with full confidentiality.
- (U) Given all these risks, I cannot stress enough how invaluable mutual cooperation remains. The evolving cyber threat scape poses many challenges to the national security community, some technical, some legal, and some with the public we serve.

- (S) Turning the discussion to the challenges facing Canada's security community, we must speak to the public environment we now operate in, particularly post-Snowden. While the Snowden revelations were certainly one of the most significant leaks of classified information in the history of the Five Eyes,

- (U) Though perhaps felt most acutely in the United States, Canadian agencies too have felt the pushback from Mr. Snowden's actions, however unfairly. One could see this in the recent debate over C-51, the *Anti-Terrorism Act*. During that debate, the activities of American agencies became caught up in the public narrative in Canada, despite the fact that the mandates and authorities of our respective agencies differ immensely. References to blanket surveillance and unauthorized meta-data collection were made, despite the fact that CSIS and our community partners do not engage in such activities in Canada.

- (U) The paradox the intelligence world has faced is that we must maintain the public's trust and confidence, while keeping our information secret. It is an unenviable task. Our review bodies have played an important role in assuring the Canadian public of the appropriateness of our activities. That said, uncontextualized leaks of information with little direct relation to Canadian activities and authorities have challenged public confidence.

- (U) Unauthorized disclosures of classified information have spawned a global debate on privacy and prompted the spread of advanced encryption throughout the Internet. Major Internet firms like Google, Apple and Facebook have now encrypted vast amounts of data on the Internet, shrouding much of the activity of all their customers.

- (U) For example, with the release of its new operating system last fall, Apple announced that its new encryption features would prevent anyone, except the device's owner, from being able to access the data stored on it. Not even Apple itself would be able to bypass a user's passcode, making it incapable of responding to warranted requests.

- (U) My fellow Director at the FBI in the United States, James Comey, has been quite candid about the challenge his and all our agencies face, describing this steady erosion of investigative capabilities as "going dark."

- (U) The challenge of "going dark" is multi-faceted. Technology continues to transform virtually every aspect of modern society, but it is doing so at a rate that has outpaced the ability for domestic laws and for investigative tools to adapt. Due to the complexity of modern technology, there are technical barriers to accessing live communications and data that is stored on devices. These problems are further complicated by increasingly secure encryption software, and, in particular the rise of end-to-end user encryption.

- (S) Today, as a result of the borderless nature of cyberspace, these technical barriers are also being magnified by legal and jurisdictional problems.

- **(S) While encryption increases information security, it also enables the Internet-based activity of malicious actors, whether criminal, terrorist, or a hostile state, allowing them to evade the investigative techniques and network defenses.**

- **(S) To provide a pertinent example, following the attacks at the National War Memorial and Parliament Hill last October,**

- **(S) Thus far, Western governments and enterprises have responded to widespread encryption with**

- **(S) While I certainly understand why some would laud such developments, we must as a society truly think through the consequences of such technology.**

I would propose that we need to find the right balance between privacy and security. They should not be viewed as mutually exclusive.

- **(S) That said, I offer no simple policy in this regard, as these matters are ones for politicians and citizens to debate. I only wish for an informed debate that will recognize the real risks of "going dark." As Director Comey recently stated, and I paraphrase, at what cost will we create a safe that cannot be cracked?**

(S) Connected to these rapidly evolving technical challenges,

Government acts for good reasons in a deliberate and considered manner. It has an obligation to consult industries, such as those you represent here today.

- **(S) That said, such governance structures will be challenged to keep pace with the rapid changes in technology. New communications technologies are invented regularly and grow in popularity, sometimes within months.**

- **(S) Ladies and gentlemen,**

- **(U) In addition to these technical concerns, cyberspace is still very much the Wild West – international law has simply not caught up to all the issues involved. There are not yet comparable and established laws for cyberspace which are recognized and widely adhered to. This leaves both Governments and the private sector little choice but to manage risks.**

- **(U) The chaotic and often anonymous nature of the internet has allowed these actors to flout the rules that have largely buttressed international systems of global trade and respect for intellectual property. An even greater level of anonymity through virtually impregnable encryption would represent a great risk to both commerce and national security. The national security community and our friends in law enforcement will continue to do our part in countering this threat and criminality, but, I would stress again the cooperation required to ensure our mutual security.**

- **(U) Changing the cost/benefit calculations for these actors who engage in such activities is a joint responsibility and will help maintain trust in systems of global governance and commerce. Such common rules are the bedrock to global finance and trade. Without such rules and regulatory certainty, businesses such as yours cannot thrive, trade would suffer, and the Canadian economy would not progress.**

- **(U) With that I will conclude, and, I look forward to your questions.**

CSIS National Security Special Brief

Rapport spécial du SCRS sur les enjeux de sécurité nationale

- CNSSB 5/18
- March 1, 2018

TOP SECRET CEO

RUSSIAN CYBER-ACTORS CONTINUE TO TARGET CANADIANS AND OLYMPIC-RELATED ENTITIES

On February 7, 2018, two days before the start of the Pyeongchang Winter Olympic Games, the Russian military intelligence (GRU)-attributed Fancy Bear's Hack Team (FBHT) claimed to leak files from the Canadian non-profit Own the Podium, an organization dedicated to improving the medal performances of Canadian Olympic and Paralympic athletes.

The aforementioned activities targeting Canadians coincide with a highly aggressive surge of GRU cyber-operations against other Olympic-related targets.

On February 24, 2017, the *Washington Post* reported that two unnamed US intelligence officials revealed that GRU hackers accessed as many as 300 Olympics-related computers in South Korea and attempted to cover up their tracks by using North Korean IP addresses, among other tactics.

CSIS National Security Special Brief

Rapport spécial du SCRS sur les enjeux de sécurité nationale

CNSSB 8/18
March 12, 2018

TOP SECRET CEO

This document is for the information of the following only: / Le présent document est transmis uniquement aux personnes suivantes :

- Minister of Public Safety, National Security and Intelligence Advisor Mr. Daniel Jean, Deputy Minister of Public Safety Canada Mr. Malcom Brown, Communications Security Establishment Chief Ms. Bossenmaier, Deputy Minister of Global Affairs Canada Mr. Ian Shugart, and Assistant Secretary – Security and Intelligence Ms. Caroline Xavier

POISONING OF FORMER RUSSIAN MILITARY INTELLIGENCE OFFICER

Background

This assessment is based on information as of March 12, 2018;

On March 5, 2018, media reported that former Russian military intelligence (GRU) officer Sergey Skripal, along with his daughter, were in critical condition after coming into contact with an unidentified substance. They were both found unconscious on a bench outside a shopping centre in Salisbury, United Kingdom (UK). There are conflicting reports as to whether the victims were poisoned at the shopping centre or at Sergey Skripal's home nearby. On March 7, 2018, UK authorities announced that Skripal was deliberately poisoned with a nerve agent in a case that police are now treating as attempted murder. The following day, UK authorities announced that 21 other people (including one police officer) have been treated for exposure related to this incident. The two primary victims remain in critical but stable condition, and the responding police officer in serious but responsive condition. On March 9, 2018, approximately 180 specially trained troops were deployed in the area with large scale decontamination and detection equipment to deal with the contamination. UK authorities indicate that scientists have identified the toxin used but they are not disclosing the identity to the public at this time. It is speculated in media reporting that the identity of the substance may be classified.

Sergey Viktorovich Skripal was arrested in Russia in 2006, and later convicted of providing the British Secret Intelligence Service (BSIS/MI6) with the identities of Russian Intelligence Services (RIS) agents working undercover in Europe. In July 2010, Skripal was one of four prisoners released by Moscow in exchange for ten Russian Foreign Intelligence Service (SVR) Illegals arrested by the Federal Bureau of Investigation (FBI) in June 2010. Skripal was later flown to the UK.

This document constitutes a record which may be subject to exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service."

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Since disclosure of information contained in this document might be injurious to national security, the Canadian Security Intelligence Service (CSIS) objects to its disclosure before a court, person or anybody with jurisdiction to compel its production or disclosure. The CSIS may take all steps pursuant to the *Canada Evidence Act* or any other legislation to protect this information or intelligence from production or disclosure.

Le présent document peut faire l'objet d'une exception obligatoire prévue par la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*. Les informations ou renseignements qu'il contient ne doivent être ni communiqués ni utilisés comme élément de preuve sans consultation préalable du Service canadien du renseignement de sécurité.

Le présent document est la propriété du Service canadien du renseignement de sécurité (SCRS). Il est transmis à votre organisme ou ministère à titre confidentiel, pour usage interne seulement. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur. Si vous êtes assujetti à une loi sur l'accès à l'information ou à d'autres lois qui vous empêchent de protéger les informations qu'il contient, veuillez en informer le SCRS immédiatement et lui retourner le document.

Le présent document est la propriété du Service canadien du renseignement de sécurité et peut constituer des « renseignements opérationnels spéciaux », au sens de la *Loi sur la protection de l'information*. Il est transmis à votre organisme ou ministère à titre confidentiel. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur.

Comme la communication du présent document pourrait porter atteinte à la sécurité nationale, le Service canadien du renseignement de sécurité (SCRS) s'oppose à sa divulgation auprès d'un tribunal, d'un organisme ou d'une personne ayant le pouvoir de contraindre la production ou la divulgation de renseignements. Le SCRS prendra toutes les mesures autorisées par la *Loi sur la preuve au Canada* ou toute autre loi afin d'empêcher la production ou la divulgation de ces informations ou de ces renseignements.

- CNSSB 9/18
- March 13, 2018

TOP SECRET CEO

This document is for the information of the following only: / Le présent document est transmis uniquement aux personnes suivantes:

- National Security and Intelligence Advisor Mr. Daniel Jean, Deputy Minister of Public Safety Canada Mr. Malcom Brown, Assistant Secretary – Security and Intelligence Ms. Caroline Xavier, Communications Security Establishment Chief Ms. Greta Bossenmaier, Deputy Minister of Global Affairs Canada Mr. Ian Shugart, Deputy Minister of National Defence Ms. Jody Thomas, Chief of Defence Staff Jonathan Vance, and Commander Canadian Forces Intelligence Command Rear Admiral Scott Bishop.

Update - Poisoning Of Former Russian Military Intelligence Officer

Background

This assessment is based on information as of March 13, 2018;

On March 12, 2018, UK Prime Minister (PM), Theresa May, identified the nerve agent used in the Salisbury attack as a Russian military grade "Novichuk Agent" applied in an "unlawful use of force". The Russian Federation (RF) spokesperson, Maria Zakharova responded to PM May's statement as "a circus show in the British parliament …it's another political information campaign, based on a provocation."

This document constitutes a record which may be subject to exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service."

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Since disclosure of information contained in this document might be injurious to national security, the Canadian Security Intelligence Service (CSIS) objects to its disclosure before a court, person or anybody with jurisdiction to compel its production or disclosure. The CSIS may take all steps pursuant to the *Canada Evidence Act* or any other legislation to protect this information or intelligence from production or disclosure.

Le présent document peut faire l'objet d'une exception obligatoire prévue par la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*. Les informations ou renseignements qu'il contient ne doivent être ni communiqués ni utilisés comme élément de preuve sans consultation préalable du Service canadien du renseignement de sécurité.

Le présent document est la propriété du Service canadien du renseignement de sécurité (SCRS). Il est transmis à votre organisme ou ministère à titre confidentiel, pour usage interne seulement. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur. Si vous êtes assujetti à une loi sur l'accès à l'information ou à d'autres lois qui vous empêchent de protéger les informations qu'il contient, veuillez en informer le SCRS immédiatement et lui retourner le document.

Le présent document est la propriété du Service canadien du renseignement de sécurité et peut constituer des « renseignements opérationnels spéciaux », au sens de la *Loi sur la protection de l'information*. Il est transmis à votre organisme ou ministère à titre confidentiel. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur.

Comme la communication du présent document pourrait porter atteinte à la sécurité nationale, le Service canadien du renseignement de sécurité (SCRS) s'oppose à sa divulgation auprès d'un tribunal, d'un organisme ou d'une personne ayant le pouvoir de contraindre la production ou la divulgation de renseignements. Le SCRS prendra toutes les mesures autorisées par la *Loi sur la preuve au Canada* ou toute autre loi afin d'empêcher la production ou la divulgation de ces informations ou de ces renseignements.

This document is for the information of the following only: / Le présent document est transmis uniquement aux personnes suivantes:

- National Security and Intelligence Advisor Mr. Daniel Jean, Deputy Minister of Public Safety Canada Mr. Malcolm Brown, Assistant Secretary – Security and Intelligence Ms. Caroline Xavier, Communications Security Establishment Chief Ms. Greta Bossenmaier, Deputy Minister of Global Affairs Canada Mr. Ian Shugart, Deputy Minister of National Defence Ms. Jody Thomas, Chief of Defence Staff Jonathan Vance, and Commander Canadian Forces Intelligence Command Rear Admiral Scott Bishop.

UPDATE: POISONING OF FORMER RUSSIAN MILITARY INTELLIGENCE OFFICER

This assessment is based on information as of March 15, 2018.

Recent Developments

On March 12, 2018, UK Prime Minister (PM), Theresa May, publicly identified the nerve agent used in the Salisbury attack as a Russian military grade "Novichok Agent" applied in an "unlawful use of force". The Russian Federation (RF) has denied involvement in this incident and it refused to respond to the UK government's ultimatum to provide an explanation by midnight of March 13, 2018. In response, on March 14, 2018, the UK PM announced in Parliament a series of initial measures against Russia. These include:

- Expelling 23 RF diplomats from the UK (they have been given one week to leave);
- Increasing checks on RF-based private flights, customs and freight;
- Freezing Russian state assets where there is evidence they may be used to threaten the life or property of UK nationals or residents;
- Ministers and the Royal Family will boycott the FIFA World Cup in Russia, June – July 2018;
- Suspending all planned high-level bilateral contacts between the UK and Russia;
- Plans to consider new laws to increase defences against "hostile state activity".

Following the UK PM's announcement, RF officials declared that Russia would respond in kind to the expulsions. On March 15, 2018, RF President Vladimir Putin chaired a meeting of the RF National Security Council to discuss how to retaliate against the UK's decision to expel 23 Russian diplomats. RF Foreign Minister Sergey Lavrov stated that Russia would "act soon". According to the Russian news agency TASS, President Putin will personally choose the retaliatory measures Moscow takes against the UK.

This document constitutes a record which may be subject to exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service."

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Since disclosure of information contained in this document might be injurious to national security, the Canadian Security Intelligence Service (CSIS) objects to its disclosure before a court, person or anybody with jurisdiction to compel its production or disclosure. The CSIS may take all steps pursuant to the *Canada Evidence Act* or any other legislation to protect this information or intelligence from production or disclosure.

Le présent document peut faire l'objet d'une exception obligatoire prévue par la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*. Les informations ou renseignements qu'il contient ne doivent être ni communiqués ni utilisés comme élément de preuve sans consultation préalable du Service canadien du renseignement de sécurité.

Le présent document est la propriété du Service canadien du renseignement de sécurité (SCRS). Il est transmis à votre organisme ou ministère à titre confidentiel, pour usage interne seulement. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur. Si vous êtes assujetti à une loi sur l'accès à l'information ou à d'autres lois qui vous empêchent de protéger les informations qu'il contient, veuillez en informer le SCRS immédiatement et lui retourner le document.

Le présent document est la propriété du Service canadien du renseignement de sécurité et peut constituer des « renseignements opérationnels spéciaux », au sens de la *Loi sur la protection de l'information*. Il est transmis à votre organisme ou ministère à titre confidentiel. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur.

Comme la communication du présent document pourrait porter atteinte à la sécurité nationale, le Service canadien du renseignement de sécurité (SCRS) s'oppose à sa divulgation auprès d'un tribunal, d'un organisme ou d'une personne ayant le pouvoir de contraindre la production ou la divulgation de renseignements. Le SCRS prendra toutes les mesures autorisées par la *Loi sur la preuve au Canada* ou toute autre loi afin d'empêcher la production ou la divulgation de ces informations ou de ces renseignements.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

CSIS National Security Special Brief

Rapport spécial du SCRS sur les enjeux de sécurité nationale

CNSSB 12/18
March 29, 2018

TOP SECRET CEO

This document is for the information of the following only: / Le présent document est transmis uniquement aux personnes suivantes:

National Security and Intelligence Advisor Mr. Daniel Jean, Deputy Minister of Public Safety Canada Mr. Malcom Brown, Foreign and Defence Policy Advisor to the Prime Minister Mr. John Hannaford, Assistant Secretary – Security and Intelligence Ms. Caroline Xavier, Communications Security Establishment Chief Ms. Greta Bossenmaier, Deputy Minister of Global Affairs Canada Mr. Ian Shugart, Deputy Minister of National Defence Ms. Jody Thomas, Chief of Defence Staff Jonathan Vance, and Commander Canadian Forces Intelligence Command Rear Admiral Scott Bishop

Update: Poisoning of Former Russian Military Intelligence Officer

Background

This CNSSB (covering developments since March 15, 2018) is based on information current to March 29, 2018, 1200 EST regarding the poisoning of former Russian military intelligence (GRU) officer in Salisbury, United Kingdom (UK) on March 4, 2018.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

CSIS National Security Special Brief

Rapport spécial du SCRS sur les enjeux de sécurité nationale

CNSSB 27/18
October 4, 2018

TOP SECRET [redacted] EYES ONLY

CSIS Contributes to Public Attribution of GRU Cyber-Activities

2018 10 04

On October 4, 2018, the Governments of Canada, the United Kingdom (UK) and the Netherlands released public statements exposing and denouncing cyber-operations carried out by officers of Russia's Main Intelligence Directorate (GRU) against international organizations throughout the world. Other nations are expected to follow with their own supporting statements. On the same day, the United States Federal Bureau of Investigation (FBI) issued criminal indictments against GRU officers involved in Russian cyber-activities. Collectively, these statements call attention to the GRU's cyber activities against the Montreal-based World Anti-Doping Agency (WADA), the Organisation for the Prohibition of Chemical Weapons (OPCW), and the Canadian Centre for Ethics in Sports (CCES), among others.

This coordinated initiative is intended to send a clear and united message to the Russian government that its actions are unacceptable to the international community.

The mention of the OPCW in multiple statements is primarily a result of the Dutch expulsion of four GRU officers caught in the midst of conducting human-enabled, cyber-operations against the OPCW in The Hague on April 13, 2018.

This document constitutes a record which may be subject to exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service."

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Since disclosure of information contained in this document might be injurious to national security, the Canadian Security Intelligence Service (CSIS) objects to its disclosure before a court, person or anybody with jurisdiction to compel its production or disclosure. The CSIS may take all steps pursuant to the *Canada Evidence Act* or any other legislation to protect this information or intelligence from production or disclosure.

Le présent document peut faire l'objet d'une exception obligatoire prévue par la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*. Les informations ou renseignements qu'il contient ne doivent être ni communiqués ni utilisés comme élément de preuve sans consultation préalable du Service canadien du renseignement de sécurité.

Le présent document est la propriété du Service canadien du renseignement de sécurité (SCRS). Il est transmis à votre organisme ou ministère à titre confidentiel, pour usage interne seulement. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur. Si vous êtes assujetti à une loi sur l'accès à l'information ou à d'autres lois qui vous empêchent de protéger les informations qu'il contient, veuillez en informer le SCRS immédiatement et lui retourner le document.

Le présent document est la propriété du Service canadien du renseignement de sécurité et peut constituer des « renseignements opérationnels spéciaux », au sens de la *Loi sur la protection de l'information*. Il est transmis à votre organisme ou ministère à titre confidentiel. Il ne doit être ni reclassifié ni communiqué, en tout ou en partie, sans le consentement de l'expéditeur.

Comme la communication du présent document pourrait porter atteinte à la sécurité nationale, le Service canadien du renseignement de sécurité (SCRS) s'oppose à sa divulgation auprès d'un tribunal, d'un organisme ou d'une personne ayant le pouvoir de contraindre la production ou la divulgation de renseignements. Le SCRS prendra toutes les mesures autorisées par la *Loi sur la preuve au Canada* ou toute autre loi afin d'empêcher la production ou la divulgation de ces informations ou de ces renseignements.